КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (3), 2019
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2019.3.4252
УДК 004.056

Борсуковський Юрій Володимирович
кандидат технічних наук, професор кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, м. Київ, Україна
OrcID 0000-0003-1973-2386
Y.Borsukovskyi@kubg.edu.ua

Борсуковська Вікторія Юріївна
Укрсоцбанк ПАТ, м. Київ, Україна
OrcID 0000-0002-4929-6987
v.barsik@gmail.com

ПРИКЛАДНІ АСПЕКТИ ЗАХИСТУ АУТЕНТИФІКАЦІЙНИХ ДАНИХ

Анотація. В даній статті розглянуті питання прикладного захисту аутентифікаційних даних користувача на об'єктах критичної інфраструктури. Розглянуто процедуру використання програмних засобів та засобів шифрування з метою реалізації організаційних та технічних заходів щодо запобігання витокам аутентифікаційних даних на об'єктах критичної інфраструктури. Наведено приклад використання відкритого програмного забезпечення KeePass для створення захищеної і прозорої у використанні бази аутентифікаційних даних користувачів. Розглянуто базовий перелік рекомендованих розширень (плагінів) для використання користувачами. Врахована можливість автономної перевірки користувачами своїх діючих паролів на співпадіння із файлом хешів скомпрометованих паролів HaveIBeenPwned. Для розміщення бази даних аутентифікаційних даних і забезпечення мобільності запропоновано використовувати USB-носій з апаратним шифруванням. Запропонований підхід дозволяє користувачу використовувати для зберігання аутентифікаційних даних шифровану базу даних і використовувати автоматизовану процедуру аутентифікації додатків та веб-сервісів, мати кілька ступенів програмного та апаратного захисту, що із однієї сторони спрощує використання аутентифікаційних даних при виконанні чинних політик безпеки і зменшує ймовірність їх дискредитації, а із іншої сторони підвищує ймовірність блокування зловмисних дій третьої сторони за рахунок багатоступінчатої системи захисту. Перевірена можливість додаткового шифрування конфігураційного файлу засобами операційного оточення та можливістю використання для цих цілей сертифікату, що зберігається на eToken. Розглянута модель реалізації процедури поєднує програмне і апаратне шифрування для захисту конфіденційної аутентифікаційної інформації. Враховано практичний досвід створення типових процедур захисту конфіденційної інформації для розробки, впровадження та управління сучасними політиками інформаційної безпеки щодо питань криптографічного захисту аутентифікаційної інформації на об'єктах критичної інфраструктури.

Ключові слова: аутентифікаційні дані, криптографічний захист, шифрування, доступ, політика, кібербезпека.

1. ВСТУП

В продовження теми про використання рішень Open Source для вирішення завдань інформаційної безпеки ми розглянемо практичний приклад створення системи захисту аутентифікаційних даних користувачів [1, 2].

Відомо, що сьогодні користувачеві доводиться запам'ятовувати безліч аутентифікаційних даних. Це і паролі для робочої станції, ноутбука, електронної пошти, локальної мережі, для домашньої веб-сторінки, для доступу по FTP, паролі інтернет-сервісів (інтернет-банкінг, акаунти на форумах, веб-сайтах, месенджерах) і т.п. Цей список можна продовжувати до нескінченності.

ISSN 2663 - 4023

З одного боку, якщо це складні паролі і їх безліч, то реально їх запам'ятати неможливо. З іншого боку, якщо сумлінно виконувати вимоги служби інформаційної безпеки, то користувачеві, а тим більше адміністраторові треба надати інструмент, який би дозволяв досить просто створювати і зберігати паролі для додатків і сервісів в захищеному вигляді і в той же час мати можливість легко ними оперувати [4].

Використання в таких випадках хмарних сервісів зберігання паролів не завжди зручно, а з іншого боку, і не зовсім безпечно - останнім часом почастішали повідомлення про злом хмарних сервісів зі зберігання паролів. Відповідно, службі інформаційної безпеки потрібно вирішити задачу з пошуком «золотої середини» в триєдиних вимогах до цього інструменту «безпека-функціонал-вартість» [1, 5].

Ми розглянемо тільки принцип побудови цього інструментального рішення, а всі фінальні налаштування безпеки кожен повинен реалізувати самостійно або звернутися в групу B2iCorpUA Team для розробки конкретних політик, процедур та інструкцій [3].

Спробуємо сформулювати мінімальні вимоги з інформаційної безпеки до такого інструменту:

Твердження 1. Повинен бути забезпечений захист аутентифікаційних даних від використання сторонніми особами і зменшена ймовірність їх компрометації.

Твердження 2. Ресурс повинен бути захищений від доступу.

Твердження 3. Повинен бути зручний і оперативний доступ до паролів.

Твердження 4. Всі аутентифікаційні дані (логіни, паролі, URL і т.д.) повинні зберігатися в одній захищеній базі даних.

Твердження 5. Логіни і паролі повинні зберігатися в зашифрованому вигляді, база даних повинна повністю шифруватися.

Твердження 6. Для доступу до бази даних повинен використовуватися майстер-пароль і додаткові засоби захисту.

Твердження 7. База даних повинна зберігатися на захищеному носії.

Твердження 8. Відносно невисока вартість рішення.

Твердження 9. Процеси використання аутентифікаційних даних повинні бути, по можливості, максимально автоматизовані.

Твердження 10. Повинна бути забезпечена можливість перевірки аутентифікаційних даних на витік до хакерських баз даних.

Ще раз підкреслюємо, що це мінімальні вимоги, які повинні забезпечити комфортне виконання користувачами парольних політик і забезпечити захист самих аутентифікаційних даних від компрометації. Безумовно ми пам'ятаємо закон № 1 з 10 основних законів безпеки "Якщо ви запустили на своєму комп'ютері програму зловмисника, це більше не ваш комп'ютер" [6].

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Розглянемо один з варіантів рішень для цієї задачі. В якості вирішення ми будемо використовувати менеджер паролів KeePass і флешку з апаратним шифрування від SAFEXS. Це працююче рішення, досить гнучке, зручне і перевірене багаторічним використанням в корпоративному секторі і в особистому застосуванні.

KeePass Password Safe - безкоштовна програма (менеджер паролів), яка дозволяє зберігати всі паролі користувача, використовуючи один головний майстер-пароль. Додаток підтримує алгоритми шифрування Advanced Encryption Standard (AES (256-

біт), Rijndael) і Twofish. Є портативна версія, яку не потрібно встановлювати і можна зберігати на флешці, що важливо буде для нашого рішення. Крім того, є відкритий код програми для його аналізу і сам інтерфейс програми перекладений на 40 мов. Також програма підтримує експорт бази паролів в різні формати TXT, HTML, PDF і т.п., а також імпорт з різних форматів. Автором програми є Dominik Reichl [7].

KeePass на сьогодні вважається однією з кращих, з відкритим кодом, безкоштовних і легких у використанні крос-платформних програм для зберігання паролів. Інструкцію по роботі і повні її налаштування можна знайти на сайті розробника і на інтернет-ресурсах, присвячених налаштуванням безпечного використання KeePass [9].

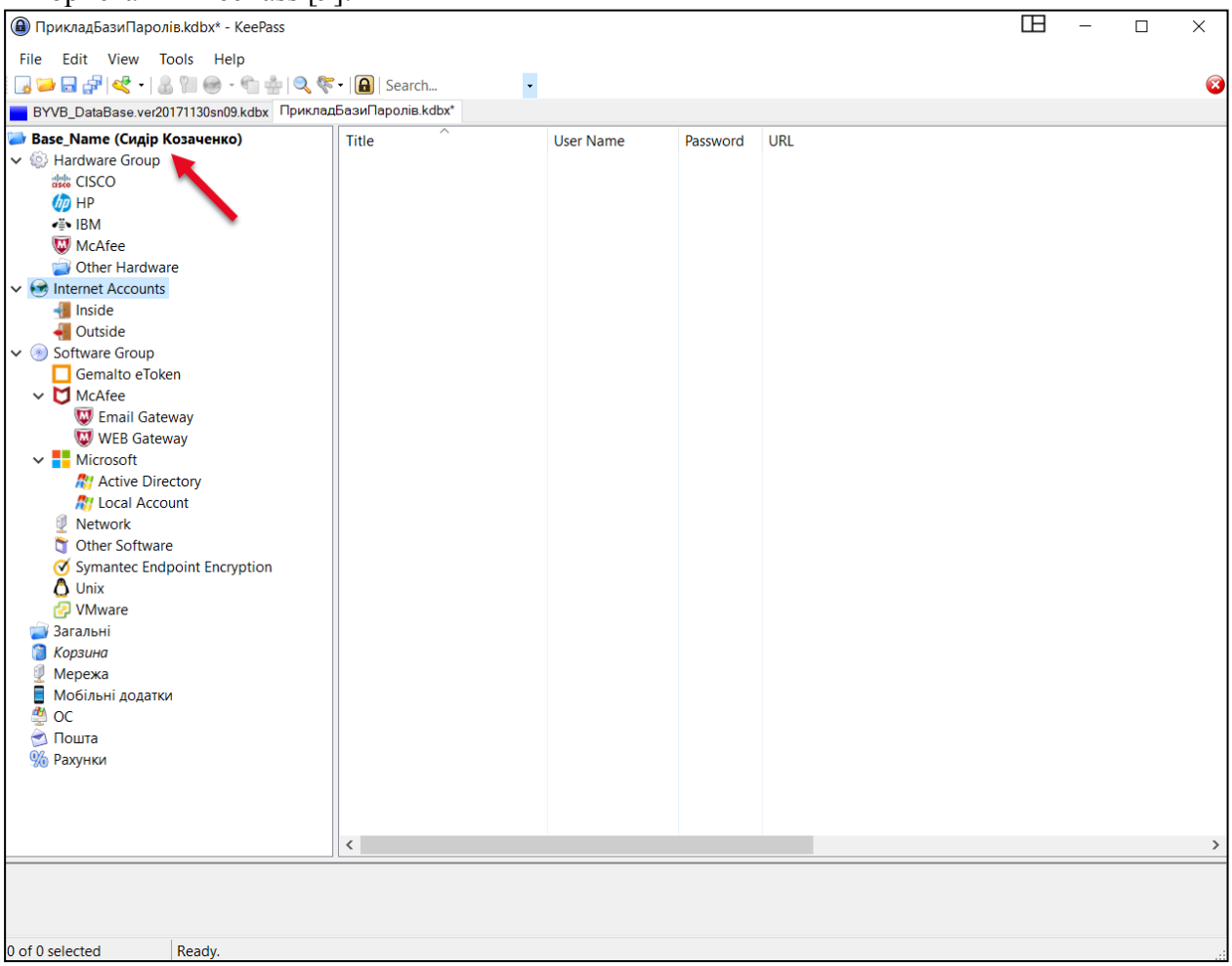

Рис. 1. Приклад структури бази даних паролів

В якості демонстраційного розглянемо приклад структури зберігання даних по групам в програмі KeePass (

Рис. 1):

Base_Name - Найменування бази даних. Кожен користувач самостійно веде свою базу даних. У базі відображаються всі облікові дані, якими володіє користувач.

Hardware Group - облікові дані на всіх технічних засобах (сервери, комутатори, роутери, маршрутизатори і т.п).

Група IBM - облікові дані для обладнання виробництва IBM.

Група Cisco - облікові дані для обладнання виробництва Cisco.

Група HP - облікові дані для обладнання виробництва HP.
Група McAfee - облікові дані для обладнання виробництва McAfee і т.д.
Internet Accounts - інтернет ресурси. У цій групі зберігаються облікові дані до інтернет ресурсів, і вони умовно розділені на дві категорії:
Outside - зовнішні ресурси, які не належать організації.
Inside - внутрішні ресурси, ресурси всередині організації.
Software Group - облікові дані в різних системах, додатках і сервісах.
Група McAfee - облікові дані в системах McAfee.
Група Web - облікові дані в системах McAfee Web Gateway.
Група Email - облікові дані в системах McAfee Email Gateway.
Група Microsoft - облікові дані в системах Microsoft.
Група Active Directory - доменні облікові дані.
Група Local Account - локальні облікові дані на серверах.
Група Network - облікові дані мережевих сервісів.
Група Unix - облікові дані в системах Linux / Unix.
Група VMware - облікові дані в системах VMware і так далі.
Цей приклад демонструє можливість групування облікових даних для використання користувачем. У кожній групі формуються облікові записи для доступу до конкретного устаткування або програмного забезпечення (*Рис. 2*).

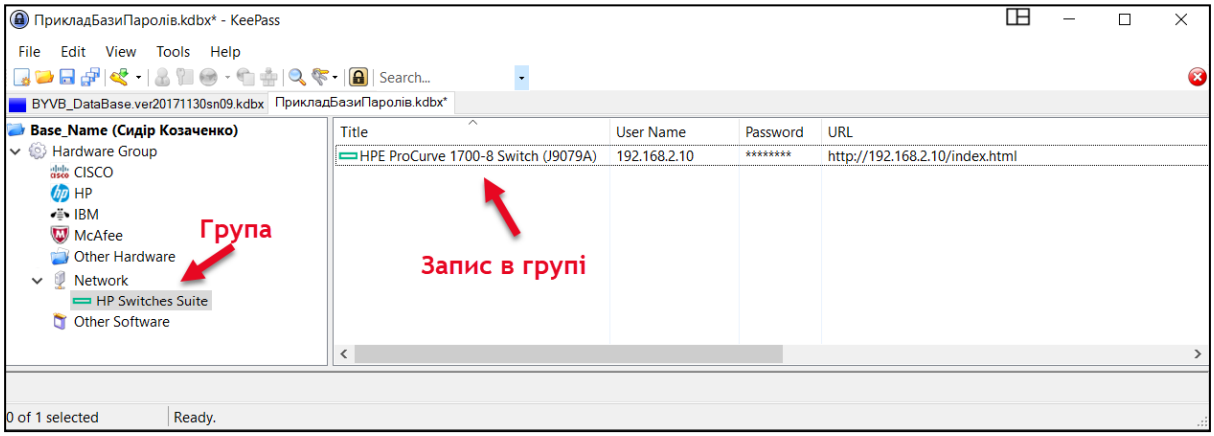

Рис. 2. Запис в групі KeePass

З метою автоматизації частини процесів і спрощення роботи користувачів існує можливість використання плагінів (plugins). На **Помилка! Джерело посилання не знайдено.** приведено перелік плагінів, який може бути рекомендовано до використання користувачам:

ISSN 2663 - 4023

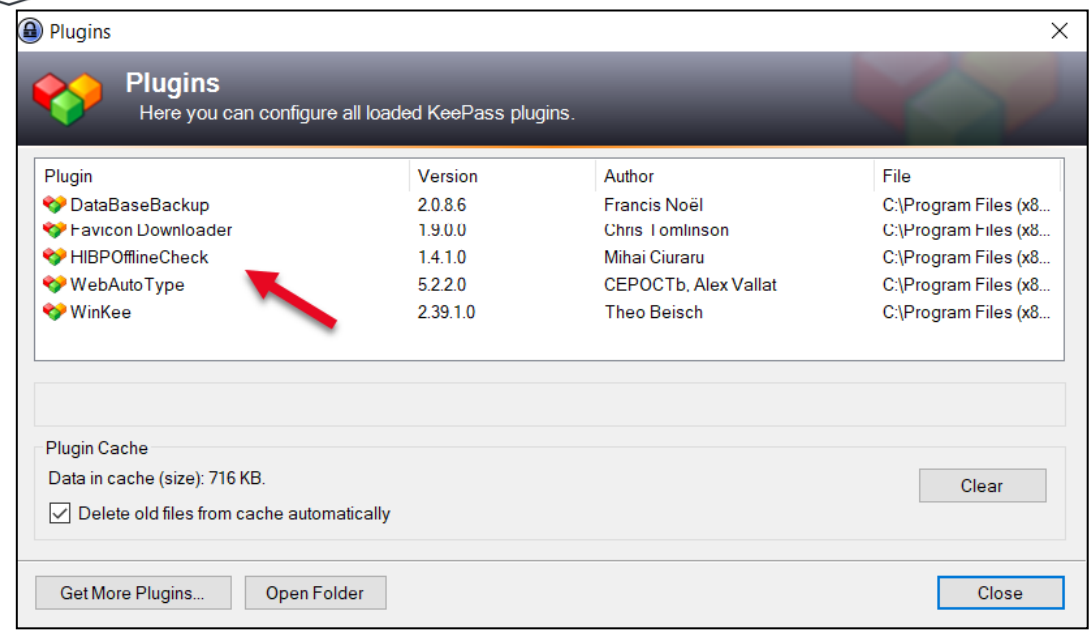

Рис. 3. Рекомендований перелік плагінів

DataBaseBackup – допомагає в автоматичному режимі створювати резервну копію бази дних.

FaviconDownloader – цей плагін завантажує та зберігає favicons (позначки). Favicons це маленький значок/логотип, який використовується для ідентифікації багатьох веб-сайтів, які зазвичай відображаються в адресному рядку браузера, списку закладок і на вкладках.

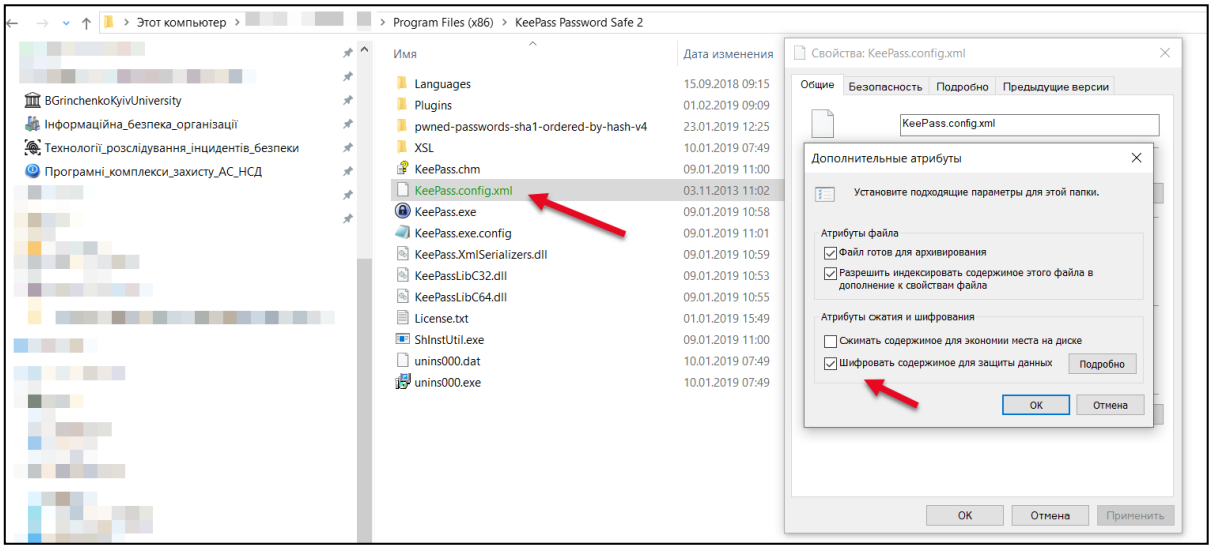

Рис. 4. Шифрування конфігураційного файлу

ISSN 2663 - 4023

HIBPOfflineCheck - цей плагін виконує автономні перевірки діючих паролів бази даних щодо файлу скомпрометованих паролів в HaveIBeenPwned passwords.

WebAutoType - цей плагін дозволяє виконувати автоматичний запуск на основі поточної URL-адреси веб-браузера замість заголовка вікна. Підтримуються різні браузери (Internet Explorer, Firefox, Opera, Chrome, ...).

WinKee – плагін допомагає безпечно автоматизувати запуск ПЗ KeePass. WinKee окремо шифрує, зберігає і отримує облікові дані доступу до бази даних KeePass у файлі конфігурації KeePass (KeePass.config.xml). Пароль та ключовий шлях до файлу будуть зашифровані на основі облікових даних облікового запису Windows. Тому кожен, хто має доступ до конкретного облікового запису користувача і має ключовий файл бази даних WinKee може отримати доступ до бази даних KeePass по спрощеній процедурі аутентифікації.

Оскільки при використанні плагіна WinKee ми зберігаємо облікові дані KeePass (зашифровані AES-256) в конфігураційному файлі, то для випадку його його компрометації можна використовувати вбудовану в операційну середу функцію шифрування за допомогою згенерованого сертифікату (*Рис. 4***Помилка! Джерело посилання не знайдено.**). Зрозуміло, що сертифікат краще зберігати на захищеному електронному носії eToken. Це дає ще один рівень захисту аутентифікаційних даних.

Тепер розглянемо рішення щодо апаратного захисту цієї бази даних. Оскільки вибиралося рішення з мінімальною ціною, то тут ми звернули увагу на захищені флеш-накопичувачі від SAFEXS [8]. Зрозуміло, що можна використовувати і захищені флеш-накопичувачі від інших виробників - Sandisk, Kingston, Transcend і ін. Тут служба інформаційної безпеки самостійно може визначати співвідношення параметрів «вимоги-функціонал-вартість».

Safexs Protector XT (*Рис. 5*) це новинка від європейського виробника Ctwo Products AB - інструмент для захисту даних в компактному формфакторі USB-накопичувача, має великий функціонал безпеки для захисту від несанкціонованого доступу, вірусів і втрати даних. Safexs Protector це один з накопичувачів з функцією Password Rescue, що дозволяє користувачеві відновити забутий пароль (потрібне включення цієї функції).

Рис. 5. Safexs USB 3.0 Protector XT

Надміцний корпус - зроблений з надзвичайно міцного сплаву, Safexs Protector XT призначений для використання в екстремальному оточенні MIL-STD-810F specification (**Помилка! Джерело посилання не знайдено.**), сертифікований та перевірений відповідно до вимог FIPS 197 (AES), NIST SP 800-38F (XTS), NIST SP 800-38A (ECB) Compliant.

ISSN 2663 - 4023

При роботі надається досить зручний інтерфейс з відповідними вкладками: Login, My Files, Backup and Share, Antivirus, Timer Settings, Auto-Destruct (*Рис. 6*).

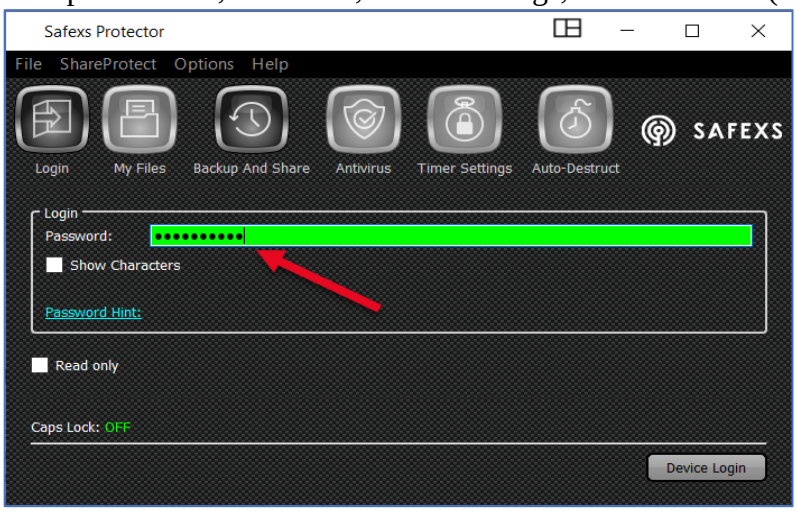

Рис. 6. Екран входу Safexs Protector

Safexs Protector XT має справжню міжплатформову підтримку, що дозволяє легко користуватися ним на комп'ютерах під управлінням Windows, Mac і Linux. Компактний форм-фактор, легкість у використанні, надзвичайна надійність і висока швидкість порту USB 3.0 робить Safexs Protector XT кращим вибором для організацій, які шукають спосіб захистити свою важливу інформацію. Safexs Protector XT оснащений вбудованою програмою ShareProtect для безпечного резервного копіювання та віддаленого доступу.

Можливості та переваги Safexs Protector XT:

256-бітове AES-шифрування в режимі XTS - апаратне шифрування. Відповідність FIPS 197.

Служба Password Rescue - функція відновлення пароля без ризику для даних (якщо вона активована).

Резервне копіювання даних - створення зашифрованої і захищеної паролем резервної копії даних на комп'ютері, NAS або хмарі.

Share Protect - портативне рішення безпеки для обміну даними, яке дозволяє легко зашифрувати файли, щоб ділитися ними з колегами і партнерами.

Функція самознищення - можливість встановити час і дату, по спливанні яких дані на пристрої будуть автоматично знищені.

Швидкість - переміщення даних відбувається за допомогою USB 3.0.

Захист від брутфорс-атаки - перебір всіх комбінацій пароля за допомогою спеціальних хакерських програм. Для введення вірного паролю надається тільки 10 спроб. При перевищенні цих обмежень всі дані на пристрої автоматично видаляються.

Антивірусний захист - річне подовження підписки.

Здатність до оновлення - регулярно з'являються нові прошивки, що містять нові функції.

З точки зору додаткового захисту інформації, яка реалізована в SAFEXS, може бути функція таймера і функція резервного копіювання і обміну даними. Захищена область флешки може автоматично закриватися після закінчення встановленого часу неактивності користувача. Корисна функція для тих, хто любить залишати USB-носій в комп'ютері. Ця функція дозволяє автоматично закрити захищену область після кінчення тайм-ауту, блокувати комп'ютер, здійснити вихід користувача, вимкнути комп'ютер (*Рис. 7*).

ISSN 2663 - 4023

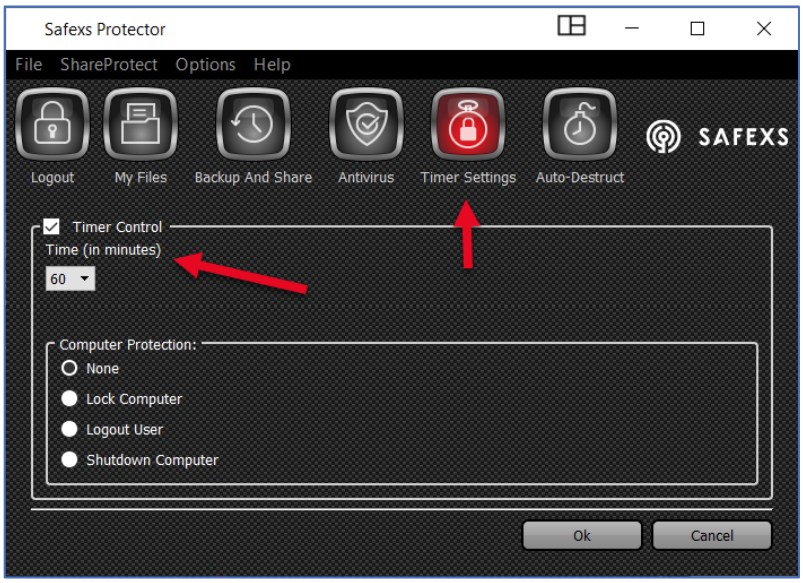

Рис. 7. Функція Timer Settings

Функція резервного копіювання і обміну даними (Backup And Share) дає ще одну сервісну функцію - це створення зашифрованого архіву з базою паролів і шифрованих файлів, при необхідності обміну конфіденційними даними між користувачами (*Рис. 8*). Шифрування файлів досить затребувана функція в роботі не тільки простих користувачів, а й системних адміністраторів. В цьому плані SAFEXS дозволяє мати готовий інструмент завжди під рукою.

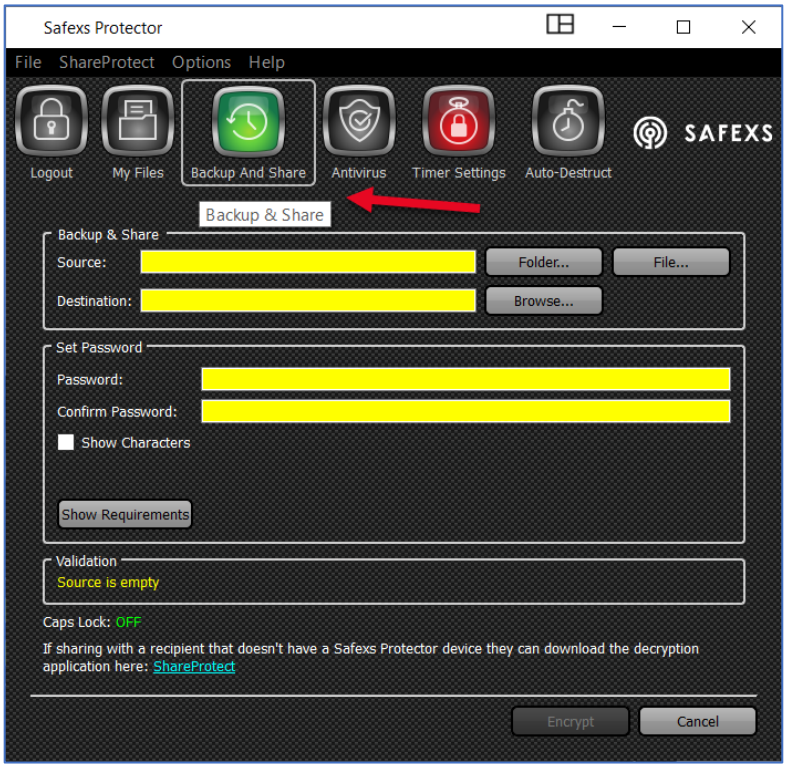

Рис. 8. Функція Backup And Share

ISSN 2663 - 4023

Дуже ефективним може бути, з точки зору служби інформаційної безпеки, активація функції автоматичного знищення даних по закінченню встановленої тимчасової точки (Auto-Destruct) - дозволяє автоматично знищити всі конфіденційні дані, якщо встановлені дата і час минули (*Рис. 9*).

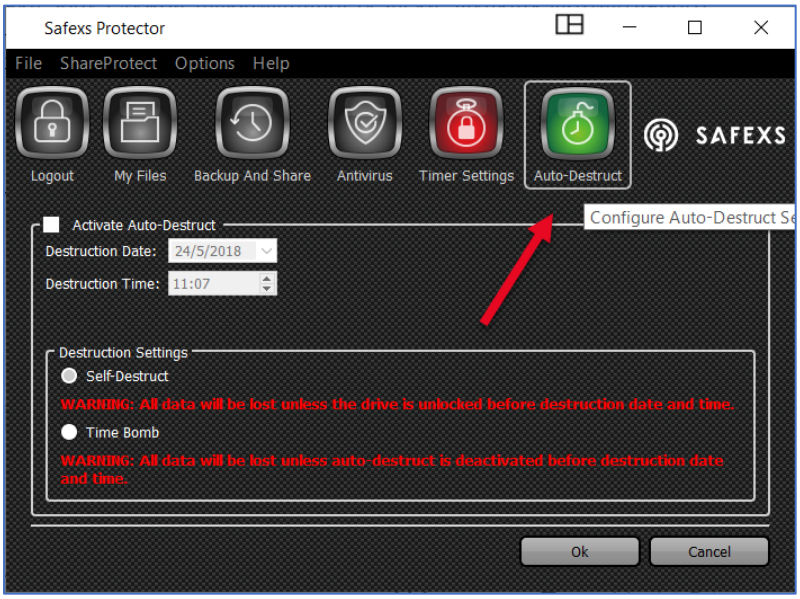

Рис. 9. Функція Auto-Destruct

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Таким чином, об'єднуючи два рішення - сервіс для зберігання паролів KeePass (Open Source) з програмним шифруванням і апаратний захист (SAFEXS) ми забезпечуємо можливість безпечного зберігання аутентифікаційних даних користувачів.

При цьому пам'ятаємо правило, що при правильних налаштуваннях KeePass зламати хороший та складний пароль за допомогою брутфорса (перебору паролів) досить складно. Єдиний спосіб швидко зламати пароль KeePass це використовувати клавіатурний шпигун для перехоплення майстер-пароля або використовувати методи соціальної інженерії [9]. З іншої сторони, використовуючи апаратне шифрування USB-накопичувача та додаючи в процедуру використання аутентифікаційних даних штатні засоби шифрування ключових та конфігураційних файлів, ми блокуємо або значно ускладнюємо переваги від перехоплення майстер-пароля при спробах отримання доступу до бази аутентифікаційних даних.

Переваги такого комплексного підходу до збереження та використання аутентифікаційних даних очевидні - ми поєднуємо програмне і апаратне шифрування для захисту конфіденційної аутентифікаційної інформації. Крім того, для парольних політик, які формує служба інформаційної безпеки, ми даємо інструмент, який дозволяє виконувати вимоги щодо цих політик. В результаті виграють обидві сторони - служба інформаційної безпеки, оскільки починають виконуватися її вимоги, і користувачі, оскільки їм надається інструмент для виконання цих вимог.

ISSN 2663 - 4023

Сформовані рекомендації та вимоги щодо прикладних аспектів використання Open Source ПЗ для захисту аутентифікаційних даних можуть бути використані при розробці політик захисту інформаційних активів на об'єктах критичної інфраструктури.

Подальші дослідження варто зосередити на створенні та впровадженні типових політик, процедур та рекомендацій щодо комплексного захисту інформаційних активів на об'єктах критичної інфраструктури як опорних точок для побудови оптимізованих по вартості і функціоналу систем інформаційної та кібернетичної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Ю. Борсуковський, "Визначення сучасних вимог до створення політики управління доступом корпоративних користувачів", Сучасний захист інформації, №. 4, стор. 5-9, 2016. Available: http://journals.dut.edu.ua/index.php/dataprotect/about. [Accessed 22 March 2019].

[2] Ю. Борсуковський, В. Бурячок та П. Складанний, "Аналіз сучасних вимог до створення парольних політик корпоративних користувачів", Сучасний захист інформації, №. 3, стор. 72-75, 2016. Available: http://journals.dut.edu.ua/index.php/dataprotect/about. [Accessed 22 March 2019].

[3] Borsukovskyi, Y. та Borsukovska, V. (2018). Model for cryptography protection of confidential information. Engineering sciences: development prospects in countries of Europa at the beginning of the third millennium. 1st ed. Stalowa Wola, Poland: Economics College, стор.43-63.

[4] NIST Special Publication 800-63-3. [Online] Available at: https://pages.nist.gov/800-63-3/sp800-63-3 [Accessed 4 Mar. 2019].

[5] Банки не готовы противостоять нарушителям во внутренней сети. [Online] Available at: https://www.anti-malware.ru/news/2018-06-05-1447/26454.

[6] Десять непреложных законов безопасности. [Online] Available at: https://technet.microsoft.com/ru-ru/library/cc722487.aspx [Accessed 4 Mar. 2019].

[7] KeePass Password Safe. [Online] Available at: https://keepass.info/ [Accessed 4 Mar. 2019].

[8] Secure Flash. [Online] Available at: https://memory.net.ua/flash/secure-flash/filter/dostupnist/dostupnii-zi-skladu/product-line/encrypted-usb-flash-drives.html [Accessed 4 Mar. 2019].

[9] Как пользоваться KeePass и защитить свои пароли?. [Online] Available at: http://www.spy-soft.net/kak-polzovatsya-keepass/ [Accessed 4 Mar. 2019].

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (3), 2019
ISSN 2663 - 4023

Yurii V.Borsukovskyi
PhD in technical sciences, professor of the Department of Information and cyber security
Borys Grinchenko Kyiv University, Ukraine
OrcID: 0000-0003-1973-2386
Y.Borsukovskyi@kubg.edu.ua

Victoria Y.Borsukovska
PJSC "Ukrsotsbank", Security Department, Kyiv, Ukraine
OrcID: 0000-0002-4929-6987
v.barsik@gmail.com

APPLICABLE ASPECTS OF AUTHENTICATION DATA PROTECTION

Annotation. This article covers the issues of applicable user`s authentication data protection at critical infrastructure objects. It considers the procedure for software and encryption facilities in order of application of organizational and technical methods to prevent loss of authentication data at critical infrastructure objects. The Article provides examples for use of open source software KeePass to create the protected and transparent in use of user`s authentication database. The Article provides the basic list of recommended extensions (plugins) for users. Considers the possibility of users` autonomous verification of their acting passwords on matching compromised passwords hash file HaveIBeenPwned. USB-carrier with hardware encryption is proposed for authentication database and ensures its mobility. Suggested provides the user with encrypted database to store the authentication data, and use the automatic procedure for authentication of applications and web-services, have few levels of software and hardware protection, which on one hand simplifies the use of authentication data in execution of applicable security policies and reduce the feasibility of its discreditation, and on the other hand increase the feasibility to block the abusive actions of third parties by means of multi-level protection system. Checked the ability for additional encryption of configuration file by means of runtime environment and ability to use the certificate which is stored at eToken. The provided model for procedure implementation combines the software and hardware encryption to protect the confidential authentication data. It considers the practical experience for creation of model procedures for confidential information protection to develop, implement and manage the modern policies of informational security related to cryptographic protection of authentication data at critical infrastructure objects.

Key words: authentication data, cryptographic protection, encryption, access, policy, cyber security.

REFERENCES

[1] Borsukovskyi, Y. (2016). Determination of Modern Requirements for Development of Corporate Users` Access Control Policy / Modern Information Protection. № 4, pp.5-9.
[2] Borsukovskyi, Y., Buriachok, V. and Skladaniy, P. (2016). Analysis of Modern Requirements for Development of Corporate Users` Passcodes Policy, Modern Information Protection. № 3, pp.72-75.
[3 Borsukovskyi, Y. and Borsukovska, V. (2018). Model for cryptography protection of confidential information. Engineering sciences: development prospects in countries of Europa at the beginning of the third millennium. 1st ed. Stalowa Wola, Poland: Economics College, pp.43-63.]
[4] NIST Special Publication 800-63-3. [Online] Available at: https://pages.nist.gov/800-63-3/sp800-63-3 [Accessed 4 Mar. 2019].
[5] Banks Are Not Ready to Resist Internal Network Abusers at. [Online] Available at: https://www.anti-malware.ru/news/2018-06-05-1447/26454.
[6] Ten Immutable Laws of Security. [online] Available at: https://technet.microsoft.com/ru-ru/library/cc722487.aspx [Accessed 4 Mar. 2019].
[7] KeePass Password Safe. [Online] Available at: https://keepass.info/ [Accessed 4 Mar. 2019].
[8] Secure Flash. [Online] Available at: https://memory.net.ua/flash/secure-flash/filter/dostupnist/dostupnii-zi-skladu/product-line/encrypted-usb-flash-drives.html [Accessed 4 Mar. 2019].
[9] How to Use the KeePass and Protect Your Passwords?. [online] Available at: http://www.spy-soft.net/kak-polzovatsya-keepass/ [Accessed 4 Mar. 2019].